UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 15250 Stafford Street, City of Industry, California 91744 as Described in Attachment A-1	)	Case No. **2:22-MJ-01604**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 501, 542, 545, 371	manufacture, sell, or possession with intent to sell counterfeit postage stamps; entry of goods by means of false statements; smuggling goods into the United States; conspiracy

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of_____days (*give exact ending date if more than 30 days*:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Mark White

Applicant's signature

Mark White, USPIS Postal Inspector

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

City and state: Los Angeles, CA

Hon. Michael R. Wilner, U.S. Magistrate Judge

Printed name and title

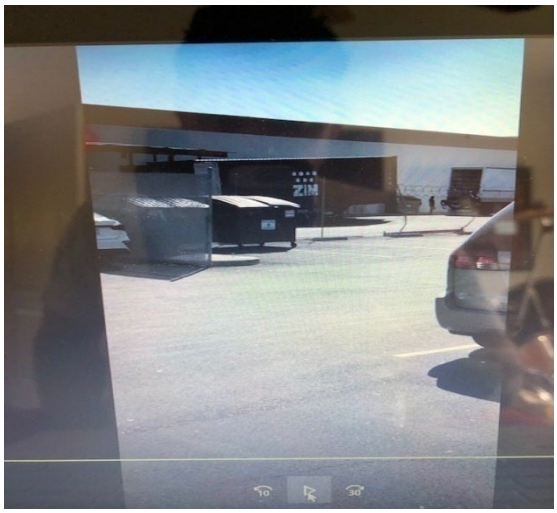
AUSA: Dominique Caamano (x0492)

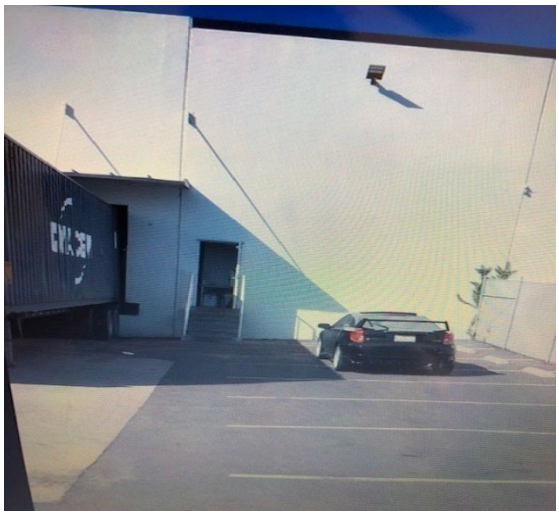
ATTACHMENT A-1

PREMISES TO BE SEARCHED

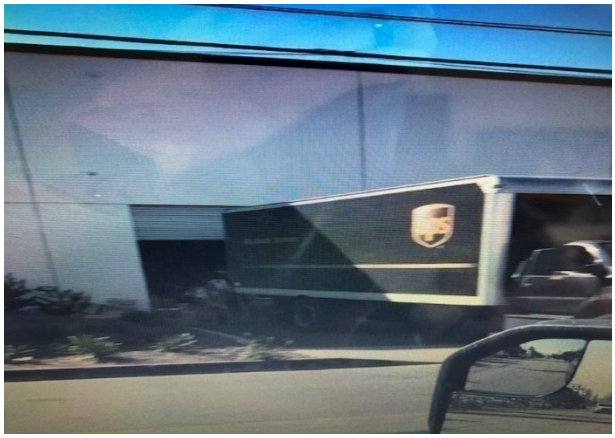
The premises located at 15250 Stafford Street, City of Industry, California 91744 ("SUBJECT PREMISES"). The SUBJECT PREMISES is further described as a "warehouse" structure with white/beige stucco with blue or black trim on top. There is a white security gate near the front entrance off Stafford Street. The number "15250" is affixed above this white security gate at the top of the building.

There is an additional gate entrance on the east side of the complex used for semi-trailer truck access. This truck unloading area is surrounded by a dilapidated barbed wired fence. There is a white pedestrian door within the unloading area leading into the warehouse.





There is an additional truck unloading area on the North side of the warehouse on Stafford Street. This area is secured by a metal garage door.



The SUBJECT PREMISES includes (a) all rooms, any attics, basements, porches, containers, and safes in the SUBJECT PREMISES; (b) any garages, carport, storage space or outbuildings designated for the occupant of the SUBJECT PREMISES; and (c) any digital devices found at the SUBJECT PREMISES.

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 501 (manufacture, sell, or possession with intent to sell counterfeit postage stamps); 18 U.S.C. § 542 (entry of goods by means of false statements); 18 U.S.C. § 545 (smuggling goods into the United States); 18 U.S.C. § 371 (conspiracy), collectively the ("SUBJECT OFFENSES"), namely:

a. Any and all altered, forged, counterfeited, raised, or falsely made postage stamps;

b. Any and all receipts regarding the sale or purchase of postage stamps;

c. Records, documents, programs, applications, or materials relating to postage stamps;

d. Any and all tools or instruments used to manufacture, sell, or otherwise distribute postage stamps;

e. Data, records, documents, or information (including electronic mail and messages) pertaining to obtaining, possessing, using, or transferring funds to bank accounts, such as names, addresses, phone numbers, credit and debit card numbers, security codes, bank account and other financial institution account numbers, Social Security numbers, email addresses, IP addresses, as well as PIN numbers and passwords for financial institutions or internet service providers;

f. Records, documents, programs, applications, or

materials pertaining to any bank accounts, credit card accounts, or other financial accounts, including applications for, or use of, credit or debit cards, bank accounts, or merchant processor accounts;

g. Data, records, documents (including e-mails), or information reflecting or referencing purchases of merchandise, securities, electronic currency, and other valuable things;

h. Records, documents, programs, applications, materials, or communications concerning efforts to track parcels sent via the United States Postal Service, including communications with the United States Postal Service;

i. Any altered, counterfeit, or fraudulent identifications, checks, access devices, monetary instruments, or other official documents, including postage stamps;

j. U.S. currency in excess of $1,000, including the first $1,000 if more than $1,000 is recovered, bearer instruments worth over $1,000 (including cashier's checks and traveler’s checks);

k. Any tools or equipment, such as computers, software, printers, scanners, embossing machines, credit card readers or encoders, washing chemicals, or imprinting tools, used or intended to be used to alter, counterfeit, or create fraudulent checks, access devices, or other monetary instruments, including postage stamps;

l. Records of off-site storage locations, including safe-deposit box keys, records, receipts, Commercial Mail Receiving Agencies, building or office space, or receiving mail

at someone else's address; or rental agreements for storage facilities;

m. Indicia of occupancy, residency or ownership of the premises being searched and things described in the warrant, including forms of personal identification, records relating to utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease of rental agreements, addressed envelopes, escrow documents, keys, letters, mail, canceled mail envelopes, or clothing;

n. Records and communications pertaining to knowledge of export/import statutes and regulations, such as rules pertaining to economic sanctions, including records and communications pertaining to particular investigations by law enforcement, financial institutions, or regulators, without limitation as to time;

o. Records and communications pertaining to the composition, value, and breakdown of goods imported and exported by BHL Transport INC and its affiliates, including draft documents, such as draft invoices, from 2019 to the present;

p. Records and communications pertaining to corporate structure or ownership of BHL Transport INC;

q. Records and communications pertaining to wealth and the movement of wealth since 2019, such as brokerage and financial institution statements, wire transfers, currency exchanges, deposit slips, cashiers' checks, and/or other financial documents related to depository bank accounts, lines of credit, credit card accounts, real estate mortgage initial

purchase loans or loan refinances, residential property leases, escrow accounts, the purchase, sale, or leasing of automobiles or real estate, or auto loans, and investments, or showing or referring to purchases or transactions for more than $10,000;

r. Counterfeit merchandise, and records and communications pertaining to the manufacture, sale, importation, valuation, or transportation of counterfeit merchandise;

s. Records and communications identifying current and previous employees, managers, officers, or other individuals involved in the operation of BHL Transport INC;

t. Any parcels associated with USPOST, which include BHL, BHL68, BHL&PAUL, BHL&SAM CHING, USPOST, ROCKY LEI, LEE LEE, JOBSS TECH, GREEN SHIP, and ALLSTARS, or any variation thereof, or parcels addressed to the SUBJECT PREMISES;

u. Contents of any calendar or date book stored on any of the digital devices;

v. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations;

w. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show address book information, including all stored or saved telephone numbers;

x. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers

accessed through any push-to-talk functions, as well as all received or missed incoming calls;

y. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the SUBJECT OFFENSES;

z. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the SUBJECT OFFENSES;

aa. Audio recordings, pictures, video recordings, or still captured images of United States mail or mail matter, whether opened or unopened, or relating to the collection or transfer of the proceeds of the SUBJECT OFFENSES;

bb. Audio recordings, pictures, video recordings, or still captured images which related to the SUBJECT OFFENSE; and

cc. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SUBJECT OFFENSES, and forensic copies thereof.

dd. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat (including WeChat) and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further, or store evidence of the offenses listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

7. During the execution of this search warrant, law enforcement is permitted to: (1) depress LiFei Yu or Weihao Chen's thumb- and/or fingers onto the fingerprint sensor of the digital device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of LiFei Yu or Weihao Chen's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device

in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Mark White, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of an application for warrants to search the following premises, and persons, as described more fully in Attachments A-1, A-2, and A-3:

a. 15250 Stafford Street, City of Industry, California 91744 (the "SUBJECT PREMISES"), as described more fully in Attachment A-1;

b. Lifei YU ("YU"), as described more fully in Attachment A-2;

c. Weihao Chen ("CHEN"), as described more fully in Attachment A-3;

2. The requested search warrants seek authorization to seize evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 501 (manufacture, sell, or possession with intent to sell counterfeit postage stamps); 18 U.S.C. § 542 (entry of goods by means of false statements); 18 U.S.C. § 545 (smuggling goods into the United States); 18 U.S.C. § 371 (conspiracy), (collectively the "SUBJECT OFFENSES"), as described more fully in Attachment B, which is incorporated herein by reference. Attachments A-1, A-2, A-3, and B are incorporated herein by reference.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses with personal knowledge of the events and

circumstances described herein. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence, instrumentalities, and contraband of the SUBJECT OFFENSES are located in the SUBJECT PREMISES or on YU and/or CHEN.

II. BACKGROUND OF AFFIANT

4. I am a Postal Inspector with the United States Postal Inspection Service ("USPIS") and have been so employed since August 2017. I am currently assigned to the Los Angeles Division, Mail Fraud/Revenue Investigation Team located in Long Beach, California. During my employment as a Postal Inspector, I have participated in investigations related to financial and postal-related crimes such as bank fraud, robbery, mail theft, postal-money-order fraud, and counterfeiting. My investigations of these crimes have included bank and telephone records analysis (including postal money orders), electronic and physical surveillance, search warrants, arrests, reviewing evidence from digital devices, and witness and suspect interviews. I have also spoken to experienced law enforcement agents and officers regarding their investigations of financial, counterfeiting, and postal-related crimes.

5. Previously, I was a Special Agent with the United States Secret Service in Santa Ana, California, from 2011 to 2017. As a Secret Service Special Agent, my duties included investigating violations of federal law, including fraud and related activity in connection with the fraudulent use of access devices, bank fraud, wire fraud, counterfeit United States currency, and identity theft.

6. During my tenure as a federal agent, I completed a ten-week Criminal Investigation Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia, as well as a seventeen-week training program at the United States Secret Service James J. Rowley Training Center in Beltsville, Maryland. At these institutions, my training included, among other things, techniques for investigating and combating counterfeiting, wire fraud, bank fraud, and access-device fraud.

7. I received my bachelor's degree from Florida State University and my master's degree from American Military University.

III. SUMMARY OF PROBABLE CAUSE

8. USPIS has been investigating e-commerce stamp merchant "USPOST.SHOP" ("USPOST"), which purports to be a legitimate seller of genuine USPS postal stamps, often advertising discounted prices on USPS Forever postage stamps. However, upon investigation, USPOST appears to be selling counterfeit USPS postal stamps coming from outside of the United States, including from China.

9. In at least one instance, the investigation has shown that the counterfeit stamps enter the United States through Los Angeles International Airport ("LAX"). When the stamps enter the United States, they are already pre-packaged to customers who have ordered purported USPS postal stamps from USPOST. In at least one instance, the packages to USPOST from China were to be delivered to the SUBJECT PREMISES addressed to a "BHL & Sam Ching."

10. This criminal conduct, which began on an unknown date, involves USPOST advertising the sale of genuine USPS Forever postal stamps via their e-commerce website USPOST. When consumers purchase stamps on USPOST, they receive discounted rates and avoid paying full price for USPS postal stamps from approved postal providers like the USPS. Currently, the price of a USPS Forever stamp is listed at 58 cents if used on a standard first-class letter. USPS does not offer discounted prices on USPS Forever Stamps. USPOST advertises "50% OFF US Forever Postage."

11. In many instances, customers determine the stamps to be counterfeit and initiate a return with USPOST for a refund. When customers initiate a return with USPOST, they are provided the address to the SUBJECT PREMISES for the return.

12. Furthermore, when customers purchase stamps from USPOST, the return address listed on the product label contains various company names--including "USPOST," "ALLSTARS," "BHL," "BHL68," and "BHL&PAUL," among others with the listed addresses for the companies being the address of the SUBJECT PREMISES.

13. According to my review of California Secretary of State documents, BHL Transport INC ("BHL") is listed as operating at the SUBJECT PREMISES. In addition, LIFEI YU ("YU") is listed as the Chief Executive Officer for BHL and her spouse WEIHAO CHEN ("CHEN") is listed as the Secretary. BHL appears to be associated with USPOST's online retail business activities as the company distributing the purchases from USPOST to customers.

14. On March 17, 2022, I went undercover as a USPS trainee with the daily USPS delivery driver for the SUBJECT PREMISES. At the premises, I met a woman who introduced herself as "Joanna." I asked "Joanna" if the SUBJECT PREMISES acted as a warehouse hub akin to the e-commerce business "Amazon." "Joanna" answered in the affirmative. This individual appeared to resemble a picture of YU I reviewed prior to my recorded undercover observation. During this undercover operation, USPIS picked up over 300 packages from the SUBJECT PREMISES. The outside of some of those packages included a scannable QR code, which when scanned, the USPOST website promptly appeared. I obtained consent from five customers of USPOST to open five intercepted packages. Upon review of the stamps inside the packages, the stamps being mailed to those customers were counterfeit. Given the sales of goods in this case involves products entering the United States from a foreign country, and because YU and CHEN are listed as operating BHL, which appears to be distributing the purchases on behalf of USPOST, I anticipate that YU and CHEN likely have information on their

digital devices regarding the sale and/or distribution of these counterfeit stamps.

IV. OVERVIEW OF US POSTAL STAMP SYSTEM

A. USPIS Role

15. The USPIS enforces more than 200 federal laws and investigates any crime that involves the mail, including but not limited to, investigations involving U.S. stamps.

B. USPS Postal Stamps

16. Postage stamps are affixed to a mail piece to show evidence of payment of postage. Postage is used to pay the costs involved in moving the mail from the sender to the recipient, as well as other costs. A Forever Stamp is valid for First Class Letter Mail no matter what the rate. Once purchased, a Forever Stamp is a perpetual stamp that never expires or declines in value.

17. Currently, genuine USPS postage is only printed in the United States by two authorized manufacturers/printers under tight controls and contain security features that can be field tested by local Postal Inspectors. Those authorized manufacturers/printers are Ashton Potter, located in Williamsville, New York, and Banknote Corporation of America, located in Browns Summit, North Carolina. These secure printing companies adhere to tight quality controls and apply specific security features embedded in each postage stamp per the direction of the USPS.

18. After U.S. postage stamps are printed, they are sent to USPS Stamp Fulfillment Services, located in Kansas City,

Missouri and Dulles, Virginia. The U.S. postage stamps are delivered via USPS trucks and USPS contracted drivers where the truckloads are secured with seals. Once Stamp Fulfillment Services receives the deliveries, the seals are then broken. Stamp Fulfillment Services distributes U.S. postage stamp stock to all USPS locations across the U.S. for retail sale. U.S. Post Offices send a request to Stamp Fulfillment Services to replenish U.S. postage stamp stock for sales. The replenished U.S. postage stamp stock is sent through U.S. mail to the requesting USPS locations.

19. All authentic USPS stamps contain a coat of "taggant." The authorized manufacturers/printers apply the taggant in two ways:

a. Taggant as a coating, after the image is printed.

b. Taggant in the paper, before the image is printed.

20. The easiest screening method to detect genuine stamps is to check for the presence of the UV taggant with a UV light.

21. Authentic USPS postage stamps:

a. are not produced outside of the United States.

b. are manufactured by two authorized companies, all located in the United States, and are subject to tight controls.

c. contain several security features, some of which can be determined by field personnel. Additional examination can be conducted by USPIS Forensic Laboratory personnel.

22. Counterfeit stamps have been manufactured in China and shipped to the United States for illegitimate gain.

23. USPS postage stamps are an attractive commodity in that there is a significant market for postage stamps being sold under face value.

V. BACKGROUND ON SUBJECTS AND ENTITIES

A. Business Entities

1. USPOST

24. USPOST is an e-commerce website which advertises the sale of genuine USPS Forever Postal Stamps at discounted prices. USPOST is registered as a Shopify account and not an authorized USPS stamp vendor.

25. Shopify is a subscription-based software which allows anyone to set up an online store to sell products, essentially becoming the subscriber/client's "Shipping Partner." "Myshopify.com" is not a company, but a "domain name" owned by a Shopify INC.

26. When a Shopify subscriber/client sets up an account with Shopify and their "domain name" is "USPost.com," the underlying real address becomes www.uspost.myshopify.com.

27. Subscribers/clients have the option of hiding their ".myshopify" information so customers never see it on their internet browser. Shopify clients often quickly change their e-marketplace Store's Domain. Although to change the Domain, it requires the client to "buy" a Custom Domain name, it is inexpensive ($10-$15 per year) and can be changed with "Domain Registrars" such as "GoDaddy", "Google Domains", and "Cloudflare", a Cybersecurity Provider and Content Delivery Network ("CDN"). This would provide an opportunity for USPOST

to disguise itself as an approved legitimate postal stamp vendor and not a personally owned e-commerce Shopify website.

28. When parcels are mailed via USPS, a requisite item for successful mailing is a mailing label. Labels are typically printed and affixed to the outside of the parcel and contain useful and pertinent data which assist the USPS in organizing and identifying the "who," "what," "when," and "where" included in the parcel.

29. One of those items included on a label is a six to nine digit number within the Intelligent Mail Indicia ("IMI") called the Mailer Identification ("MID"). MIDs are assigned by the USPS to a Mail Owner, Mailing Agent, or other service provider(s) who request them and identifies a specific "agent" within the mailing supply chain, including the "USER."

30. Parcels associated with USPOST, which include BHL, BHL68, BHL&PAUL, USPOST, ROCKY LEI, LEE LEE, JOBSS TECH, GREEN SHIP, and ALLSTARS, contain permit #39827 and MIDs: 90280976 or 902809677. MIDs 90280976 and 902809677 are registered to a company called PYK Global; USER "TPLX-ARLYBA(34503236)" and "TPLX-WEGRAG(34503230)" respectively, with an address registered to the SUBJECT PREMISES.

31. PYK Global is a USPS GDE (Global Direct Entry) partner and logistics company created to bridge the gap between countries, allowing for efficient and profitable commerce. Under the GDE program, the USPS established relationships with certain wholesalers (i.e., PYK Global) which tender

international inbound shipments and parcels to USPS after CBP has cleared them.

32. PYK Global has an existing contract with the USPS and has numerous MIDs assigned to it. These MIDs are used by various companies who are PYK Global customers/clients.

33. Some of these labels containing different company names and return addresses, such as "ALLSTARS," which has a return address of 1380 Stafford Street, City of Industry, CA 91744 (which address does not exist). Nevertheless, reviewed ALLSTARS parcels contain the aforementioned MIDs 902809677 or 90280976, which return to PYK Global with the "User" having the same address as the SUBJECT PREMISES.

2. BHL TRANSPORT INC.("BHL")

34. This investigation has uncovered that BHL appears associated with USPOST as the business entity that distributes the orders placed on USPOST's website.

35. On November 4, 2021, I conducted a California Secretary of State Business Search query into BHL.

36. BHL (entity number C4229828) is a domestic stock entity, listed as an international trading, logistics consulting service, and management consulting company. BHL was initially registered on January 7, 2019, and is currently considered an "active" business per the California Secretary of State website.

B. Individual Subjects

1. LIFEI YU

37. On the California State Secretary website, the electronic filing document for BHL lists YU as the Chief

Executive Officer, Director, and Agent for Service of Process, with all addresses listed on the document returning to the SUBJECT PREMISES. Although YU's name has not appeared on the packages intercepted at LAX, I conducted undercover surveillance at the SUBJECT PREMISES on March 17, 2022. During that undercover operation, I met a woman who introduced herself as "Joanna," but whose appearance resembled a photograph I reviewed of YU.

38. On August 2, 2021, YU certified the business and filing information for BHL as true and accurate via an electronic signature.

2. WEIHAO CHEN

39. CHEN is YU's spouse.

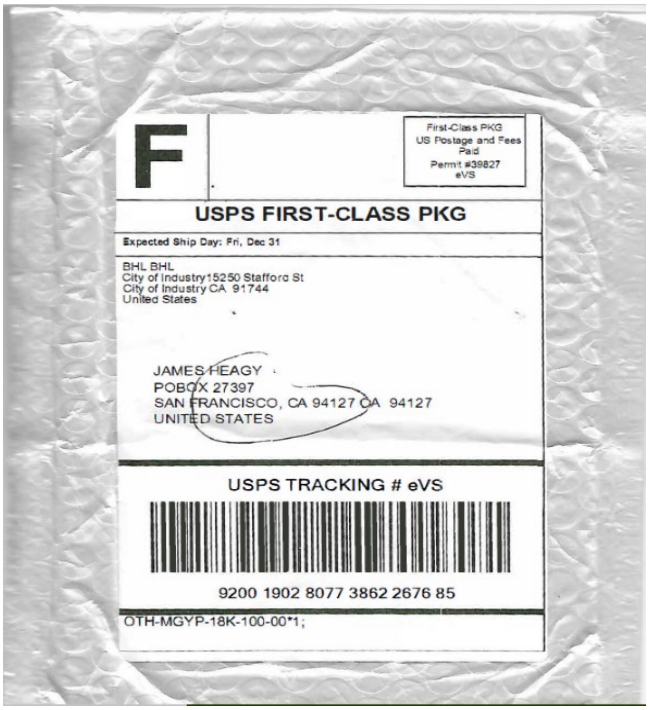
40. On the California State Secretary website, the electronic filing document for BHL lists CHEN as the Secretary with all addresses listed on the document returning to the SUBJECT PREMISES.

VI. STATEMENT OF PROBABLE CAUSE

A. USPOST Complaints

41. My investigation into USPOST began in or about November 2021. The investigation was prompted by over 71 complaints received via the USPIS "Fraud Complaint System" ("FCS"). FCS is a USPIS database that allows customers to relay pertinent postal complaints which warrant further investigation by Postal Inspectors. Once the information is entered into FCS, a complaint number is generated, and a Fraud Complaint Summary is provided to a PI for follow up.

42. On August 20, 2021, the USPIS received a fraud complaint via the FCS system. The reporting party, "J.H.," wanted to report the "sale of massive amounts of counterfeit American stamps on the internet." J.H. informed the USPIS that he made 13 purchases of rolls of 100 U.S. flag stamps over eBay via USPOSTAGE.SHOP over a period of approximately one month.[1] J.H. examined his purchases and confirmed the stamps were counterfeit with a short-wave UV light and confirmed the stamps did not possess taggant. After J.H. was able to confirm the stamps were counterfeit, he was able to receive a refund for his purchase from the USPOST eBay store. The return address on the mailing labels of his purchases were all from the SUBJECT PREMISES.



[1] As discussed below, USPOSTAGE.SHOP is associated with USPOST.

B. Counterfeit Stamp Sales Connected to SUBJECT PREMISES

43. On or about February 2022, I spoke with USPIS Inspector Dvorak in Chicago, who informed me of the following:

44. On January 12, 2022, a USPS office located in Roscoe, Illinois contacted Inspector Dvorak referencing a damaged and opened package with what appeared to be several 100 count coils of U.S. Flag postage stamps inside.[2]

45. On the same date, Inspector Dvorak retrieved and examined USPS Priority Mail Parcel 9205 5902 8096 7663 0364 17 and observed the following: the parcel weighed approximately 10 pounds, 3 ounces, and was approximately 10 ½ inches by 6 ½ inches by 5 ½ inches. The parcel was mailed on or about January 8, 2022 and addressed to C.M. at an address on Andrews Drive in Roscoe, Illinois 61073-7006. The parcel listed a return address to the SUBJECT PREMISES. The parcel had been damaged and ripped open during the mail processing, revealing numerous 100 count coils of U.S. flag forever inside.

46. On the same date, Inspector Dvorak met with C.M. at his residence to discuss the parcel. C.M. told him he had been purchasing and selling stamps online to make additional money. C.M. said he met an unidentified individual on social media and purchased the stamps for $12.00 per 100 count coil and then sold each coil for $25.00. Inspector Dvorak informed C.M. that U.S. postage stamps could only be purchased through the United States

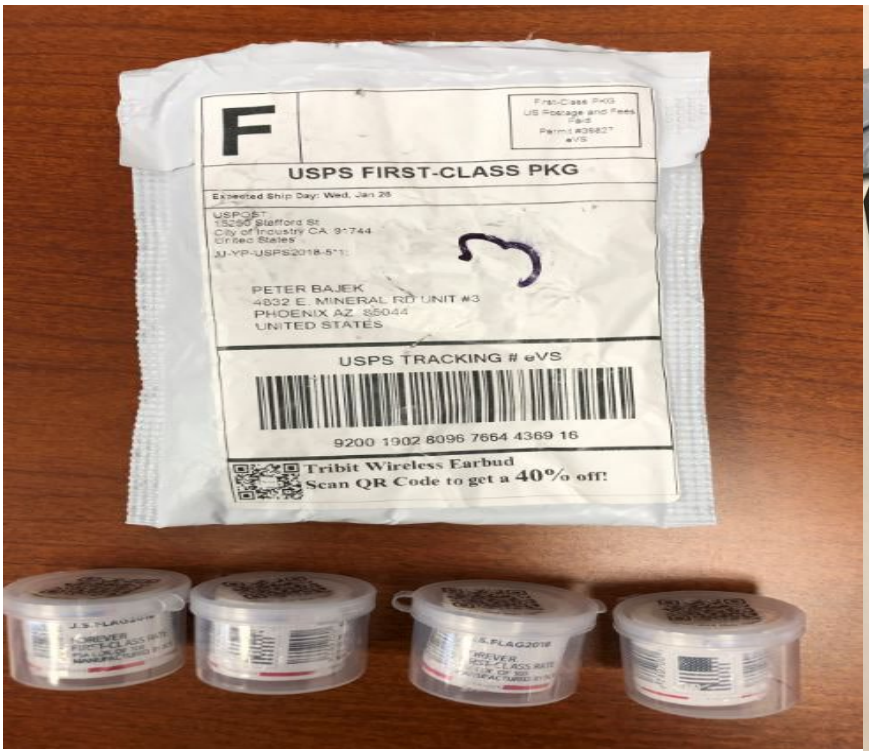
[2] Inspector Dvorak did not seek a search warrant for the open parcel.

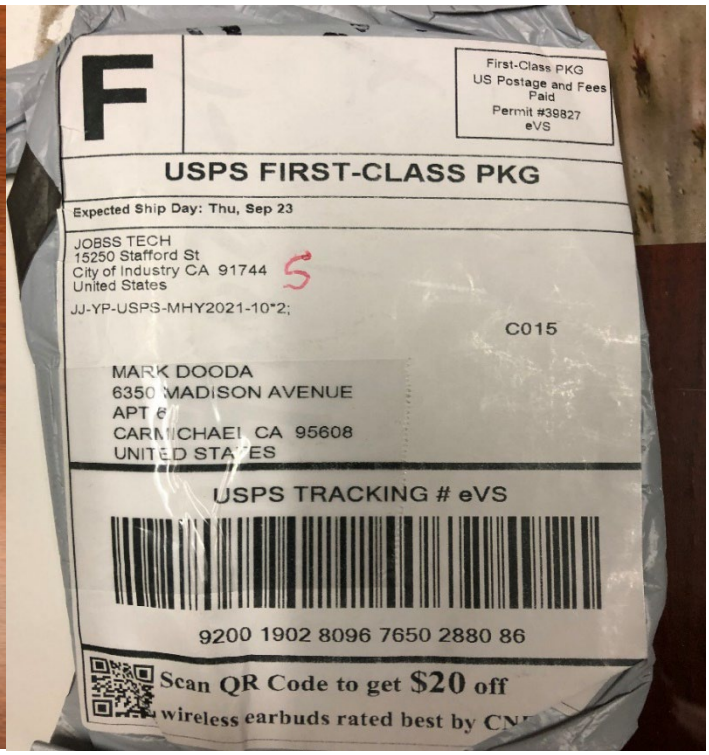
Postal Service or through an approved vendor such as a grocery store. Inspector Dvorak advised C.M. he was engaging in fraudulent activity by purchasing and selling counterfeit postage stamps and provided him a Voluntary Discontinuance Cease and Desist Agreement to that effect, which was signed and left with C.M.

47. On or about January 13, 2022, Inspector Dvorak took a random sample of two 100 count coils from the damaged area of the parcel and submitted them to the U.S. Postal Inspection Service Forensic Laboratory for analysis of authenticity.

48. On February 3, 2022, PI Dvorak received confirmation from the U.S. Postal Inspection Service Forensic Laboratory the submitted coils were determined to be "non-genuine" USPS postage.

49. During the course of the investigation, the USPIS received additional customer parcels purchased from USPOST which display the SUBJECT PREMISES listed on the outside of the parcels, including the following examples:





C. Surveillance at the SUBJECT PREMISES

50. On March 17, 2022, I conducted an undercover observation, which I recorded, at the SUBJECT PREMISES.

51. During this observation, I was outfitted as a USPS employee in training and partnered with a USPS driver, who is the daily carrier for the SUBJECT PREMISES.

52. Upon arrival, the Over-the-Road Container ("OTR") was already loaded with parcels and ready for pickup outside of a roll-up designated garage area at the SUBJECT PREMISES. The USPS driver advised that this roll-up garage area is the location for his daily pick up of parcels from the SUBJECT PREMISES.

53. As the USPS driver and I finished loading the OTR into the truck, I observed a female located at the entryway of the roll-up garage door. This unknown female appeared to be monitoring our loading of the OTR. I asked the female for her name and was told "Joanna." I asked Joanna if the warehouse was similar to an all-purpose warehouse, like Amazon (the e-commerce company), which Joanna responded in the affirmative.

54. "Joanna" appeared to very similar in appearance to YU based upon my DMV review of YU's California driver's license picture.

55. During the observation, I was able to collect a total of 325 parcels, all of which were either from companies: "ALLSTARS" or "GREENSHIP" with return addresses of 1380 Stafford Street, City of Industry, CA 91744 for "ALLSTARS" and 785 North Nantes Avenue, Los Angeles, LA Puente, CA 91744 for

"GREENSHIP". Parcels from "ALLSTARS" and "GREENSHIP" both contained permit number #39827 with MIDs "90280976" and "902809677," which are associated with PYK Global. The packages also contained QR codes, which when scanned, promptly lead me to the website for USPOST.

56. On March 21, 2022, I contacted five USPOST customers, all of whom had packages addressed to them from ALLSTARS, which I picked up during my observation, and who stated they purchased stamps online. Furthermore, I received consent from each customer to open the packages and confirm the authenticity of the stamps. The results of my field test revealed all the packages contained counterfeit stamps. Specifically, the stamps did not contain a UV taggant when examined under a short-wave UV light.

57. Furthermore, while analyzing the packages which were being sent from "ALLSTARS," I noticed the stamps were placed into a white carboard mailer. Affixed to the outside of the mailer was a circular sticker with a scannable QR code. The top portion of the sticker said "USPOST.SHOP", below that, the scannable QR code, followed by "Scan and Buy Again" written on the bottom. When the QR code was scanned, the "USPOST.SHOP" website promptly appeared.

58. Continuing on March 21, 2022, I contacted two customers who had packages addressed to them from GREENSHIP, which were intercepted by me during my observation and who stated they purchased stamps online. I observed the GREENSHIP parcels came in manilla packaging, contrast to the gray/off

white color of the ALLSTARS packaging. The GREENSHIP parcels also contained a QR code, however, when scanned it did not prompt the user to USPOST.SHOP, but rather to other e-commerce stamp websites, advertising the same discounted rate for USPS Forever Stamps, such as collectionestore.net and nicestamps.net. Both of the websites I navigated to during this analysis contained the same website instructions/verbiage as USPOST.SHOP.

59. On April 15, 2022, I attempted to conduct surveillance of ALLSTARS located at 1380 Stafford Street, City of Industry, CA 91744. I was able to confirm the address did not exist. Additionally, I did not find ALLSTARS listed on the California Secretary of State website.

60. Continuing on April 15, 2022, I attempted to conduct surveillance of GREENSHIP located at 785 North Nantes Avenue, La Puente, CA 91744. I confirmed the address to be the office of Nantes Manor Apartment Homes located in La Puente. I did not find GREENSHIP listed on the California Secretary of State website.

D. Customs and Border Patrol locate packages destined for SUBJECT PREMISES

61. On April 11, 2022, I spoke with a Customs and Border Protection Officer C. Lao regarding the detection of counterfeit stamps destined for the SUBJECT PREMISES. CBP Officer Lao informed me of the following:

62. During a routine examination, CBP Officer Lao located two shipments (a total of four boxes, two boxes for each shipment) being shipped through DHL Express Worldwide WPX

containing counterfeit stamps. CBP Officer Lao stated that the DHL packages were addressed to "BHL & Sam Ching" at the SUBJECT PREMISES from "Cindy Li" at Shenzhen Shanglade Lighting LTD of Hong Kong China. The packages were weight listed at 25.5 KG (56.2 LBS) and listed the following content material on the outside of the box: "9.7-inch Plastic Case for Tablet, Cellphone case." Inside the packages were GREENSHIP parcels, which resemble previously identified parcels that contained counterfeit stamps. I have yet to review what is inside the packages as CBP is currently processing the shipments and I have yet to receive them in my possession.

VII. TRAINING AND EXPERIENCE REGARDING FRAUD AND COUNTERFEITING.

63. Based on my training and experience and information obtained from other law enforcement officers and agents who investigate bank fraud, wire fraud, money order/check fraud, and counterfeiting offenses, I know the following:

a. It is common practice for individuals involved in fraud related schemes such as bank fraud, wire fraud, money order/check fraud, and counterfeiting offenses to possess and use multiple digital devices at once. Such digital devices are often used to facilitate, conduct, and track fraudulent transactions. Individuals who participate in bank fraud, wire fraud, money order/check fraud, and counterfeiting schemes often have coconspirators and other individuals involved in the conspiracy, and often maintain telephone numbers, email addresses, and other contact information and communications involving their coconspirators and others involved in the conspiracy in order to conduct their business. Oftentimes, they do so on their digital devices. Suspects often use their digital devices to communicate with coconspirators and others involved in the conspiracy by phone, text, email, and social media, including sending photos.

b. Individuals involved in these crimes will often funnel the proceeds from these crimes through or to the bank accounts of coconspirators or others involved in the conspiracy, often using digital devices.

c. Individuals involved in fraud related schemes, will commonly possess, and use equipment, digital devices, machinery, imprinters, solvents, phones, "cutting" utensils, printer paper, and drying machinery and other specialized tools to create altered checks, money orders, counterfeit currency, and counterfeit stamps. Software relevant to such schemes can often be found on digital devices, such as computers and phones.

These individuals will commonly store this equipment and tools used for altering checks, money orders, and counterfeit currency/stamps in safe locations that are easily accessible, such as their homes, place of business, and/or vehicles.

d. Individuals involved in these crimes will often use social media/instant messaging apps, such as WeChat, and WhatsApp to collaborate, organize, and otherwise discuss details of their crimes through, or to coconspirators, or others involved in the conspiracy, using digital devices.

e. WeChat is a social media messaging app. WeChat supports video, voice, and text data and has unique features like localized translation. Based upon my training and experience, individuals involved in counterfeiting or other fraud related activities, such as repackaging schemes, counterfeit stamp manufacturing and distribution, often use WeChat to discuss their activity or to make arrangements for pickup and delivery of such items.

VIII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[3]

64. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I

[3] As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such file's months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

65. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

66. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an

enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress Lifei Yu or Weihao Chen's, thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of Lifei Yu or Weihao Chen's face with their eyes open to activate the facial-, iris-, and/or retina-recognition feature.

d. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

IX. CONCLUSION

67. For all of the reasons described above, there is probable cause to believe that YU, CHEN, and other unknown coconspirators have committed the SUBJECT OFFENSES, and that evidence, instrumentalities, and contraband as described in Attachment B will be found in a search of the SUBJECT PREMISES and the persons described in Attachments A-1, A-2, and A-3.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ____ day of April, 2022.

_____
HONORABLE MICHAEL R. WILNER
UNITED STATES MAGISTRATE JUDGE